Service And Version detection

Nmap provides service and version detection as part of its capabilities to gather detailed information about the services running on remote systems. By default, Nmap performs version detection when scanning.

1. Attempts to determine the version of the service running on port

```
nmap -p <port_number> -sV target.com
```

In this command:

-p <port_number> specifies the target port you want to scan.

-sV instructs Nmap to perform service version detection.

target.com is the target host you are scanning.

For example, if you want to determine the version of the service running on port 80, you can use:

```
nmap -p 80 -sV target.com
```

Nmap will send specific probes to the target port and analyze the responses to try and identify the version of the service.

Keep in mind that aggressive version detection may be noisy and may be more easily detected by intrusion detection/prevention systems. Use such features responsibly and, as always, ensure you have proper authorization before scanning any network or system. Unauthorized scanning is against the law and can have serious legal consequences.

2. Intensity level 0 to 9. Higher number increases possibility of correctness:

```
nmap -sV --version-intensity <intensity_level> target.com
```

In Nmap, the -sV option is used for service version detection, and --version-intensity is used to control the intensity of version detection. The --version-intensity option allows you to specify the intensity level, which ranges from 0 to 9. The higher the intensity, the more aggressive and comprehensive the version detection will be

3. Enable light mode. Lower possibility of correctness. Faster

The `--version-light` option in Nmap is used to reduce the intensity of service version detection, making the scan less aggressive. This option is particularly useful when you want to perform version detection but with a lower impact on the target system. Here's an example:

```
nmap --version-light target.com
```

4. Enable intensity level 9. Higher possibility of correctness. Slower

In Nmap, the -sV option is used for service version detection, and --version-all is used to enable even more aggressive version detection. When you use --version-all, Nmap will attempt to detect the version of all services, even those that are considered uncommon or rarely used.

```
nmap -sV --version-all target.com
```

---

5. Remote OS detection using TCP/IP stack fingerprinting

In Nmap, the -0 option is used for OS (Operating System) detection. When you include -0 in your Nmap command, it instructs Nmap to attempt to determine the operating system of the target host based on characteristics observed during the scan.

Here's an example:

```
nmap -O target.com
```

In this command:

-0 enables OS detection.

Nmap uses various techniques, such as analyzing responses to TCP/IP stack fingerprinting, to make an educated guess about the target's operating system. However, note that OS detection is not always accurate, and it relies on patterns that may be influenced by firewalls, network configuration, or other factors.

Keep in mind the following:

Privileges: Performing OS detection typically requires root (administrator) privileges or elevated permissions on the system running Nmap.

Firewalls: The accuracy of OS detection can be affected by firewalls and other security measures that may alter or block certain packets.

Here's an example of how you might use OS detection in combination with service version detection (-sV):

```
nmap -O -sV target.com
```

This command will perform both OS detection and service version detection on the specified target.

As always, ensure you have proper authorization before conducting any network scans. Unauthorized scanning is against the law and can have serious legal consequences.

---

6. If at least one open and one closed TCP port are not found it will not try OS detection against host

In Nmap, the --osscan-limit option is used to limit the number of OS detection probes sent to a target. When this option is used, Nmap will only send a reduced number of OS detection probes in order to make the scan less intrusive and potentially avoid detection by intrusion detection systems.

```
nmap -O --osscan-limit target.com
```

7. Makes Nmap guess more aggressively

In Nmap, the --osscan-guess option is used to specify a particular type of OS detection. When you use this option, you are essentially telling Nmap to guess the operating system based on the results of the initial port scan without performing further probes. This can be useful if you want a quicker OS detection result but with potentially less accuracy compared to a more thorough OS detection.

```
nmap -O --osscan-guess target.com
```

8. Set the maximum number x of OS detection tries against a target

The `--max-os-tries` option in Nmap is used to specify the maximum number of OS detection tries against a target. OS (Operating System) detection in Nmap involves sending various probes to the target and analyzing the responses to make an educated guess about the operating system.

```
nmap -O --max-os-tries 2 target.com
```

9. Enables OS detection, version detection , script scanning, and traceroute

```
nmap -A target.com
```